LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for assigning ~~certificates/private keys~~certificates and associated private keys to a token, comprising:

accessing the token through a token reader connected to a computer system by a ~~certificate/private key~~certificate authority;

reading a token ID and a user-signature certificate from the token;

searching for a match for the token ID and the user signature certificate in an authoritative database;

creating a certificate and an associated private key, wherein the certificate and the associated private key are ~~is~~ wrapped with a public key associated with the token ID and digitally signing the ~~certificate/private key~~certificate and the associated private key using a signature certificate of the certificate authority if a match for the token ID and the user signature certificate is found in the authoritative database;

downloading the ~~certificate/private key~~certificate and the associated private key to the token; and

decrypting the ~~certificate/private key~~certificate and the associated private key using a private key stored in the token, such that the token stores at least the token ID, the private key, the user signature certificate and the certificate and the associated private key.

2. (Currently Amended) The method recited in claim 1, wherein the ~~certificate/private key~~certificate and the associated private key is a plurality of ~~certificates/private keys~~certificates and associated private keys wherein ~~that~~ at least one ~~certificate/private key~~of the plurality of certificates and associated private keys is a signature certificate for the user, an encryption ~~certificate/private key~~certificate and associated private key for the user, and a role

~~certificate/private key~~certificate and associated private key for the user wherein the role certificate includes at least one policy.

3. (Currently Amended) The method recited in claim 2, wherein the wrapping of the certificate and the associated private key with the public key of the token encrypts the certificate and the associated private key.

4. (Original) The method recited in claim 3, wherein the token is a smart card.

5. (Original) The method recited in claim 4, wherein the token ID is assigned by a token manufacturer at the time the token is created and stored in the authoritative database when assigned to a user.

6. (Currently Amended) The method recited in claim 5, wherein downloading the ~~certificate/private key~~certfficate and the associated private key to the token is done through an unsecured communications line.

7. (Currently Amended) The method recited in claim 6, wherein decrypting the ~~certificate/private key~~certificate and the associated private key using ~~a~~the private key stored in the token requires the entry of a passphrase by a user.

8. (Currently Amended) The method recited in claim ~~11~~7, further comprising:

authenticating, by the signing of the ~~certificate/private key~~certificate and the associated private key using a signature certificate of the certificate authority, that the ~~certificate/private key~~certificate and the associated private key were was issued by the certificate authority.

9. (Currently Amended) A computer program embodied on a computer readable medium and executable by a computer for assigning ~~certificates/private keys~~certificates and associated private keys to a token, comprising:

accessing the token through a token reader connected to a computer system by a certificate authority;

reading a token ID and a user signature certificate from the token;

searching for a match for the token ID and the user signature certificate in an authoritative database;

creating a certificate and an associated private key, wherein the certificate and the associated private key are ~~is~~ wrapped with a public key associated with the token ID and digitally signing the ~~certificate/private key~~certificate and the associated private key using a signature certificate of the certificate authority if a match for the token ID and the user signature certificate is found in the authoritative database;

downloading the ~~certificate/private key~~certificate and the associated private key to the token; and

decrypting the ~~certificate/private key~~certificate and the associated private key using a private key stored in the token, such that the token stores at least the token ID, the private key, the user signature certificate and the certificate and the associated private key.

10. (Currently Amended) The computer program recited in claim 9, wherein the ~~certificate/private key~~certificate and associated private key is a plurality of ~~certificates/private keys~~certificates and associated private keys wherein ~~that~~ at least one ~~certificate/private key~~of the plurality of certificates and associated private keys is a signature certificate for the user, an encryption ~~certificate/private key~~certificate and associated private key for the user, and a role ~~certificate/private key~~certificate and associated private key for the user, wherein the role certificate includes at least one policy.

11. (Currently Amended) The computer program recited in claim 10, wherein the wrapping of the certificate with the public key of the token encrypts the ~~certificate/private key~~certificate and the associated private key.

12. (Original) The computer program recited in claim 11, wherein the token is a smart card.

13. (Original) The computer program recited in claim 12, wherein the token ID is assigned by a token manufacturer at the time the token is created and stored in the authoritative database when assigned to a user.

14. (Currently Amended) The computer program recited in claim 13, wherein downloading the ~~certificate/private key~~certificate and the associated private key to the token is done through an unsecured communications line.

15. (Currently Amended) The computer program recited in claim 14, wherein the decrypting the ~~certificate/private key~~certificate and the associated private key using ~~a~~the private key stored in the token requires the entry of a passphrase by a user.

16. (Currently Amended) The computer program recited in claim 15, further comprising:

authenticating by the signing the ~~certificate/private key~~certificate and the associated private key using a signature certificate of the certificate authority that the ~~certificate/private key~~certificate and the associated private key was issued by the certificate authority.